Chapter 3
The Information Systems Security Engineering Process

Information Systems Security Engineering (ISSE) is the art and science of discovering users' information protection needs and then designing and making information systems, with economy and elegance, so they can safely resist the forces to which they may be subjected. This chapter describes an ISSE process for discovering and addressing users' information protection needs. The ISSE process should be an integral part of systems engineering (SE) and should support certification and accreditation (C&A) processes, such as the Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP). The ISSE process provides the basis for the background information, technology assessments, and guidance contained in the remainder of the Information Assurance Technical Framework (IATF) document and ensures that security solutions are effective and efficient.

3.1 Introduction

This chapter is organized into five sections, as follows:

- Section 3.1, Introduction.
- Section 3.2, Discussion of three important SE and ISSE principles.
- Section 3.3, Description of ISSE activity in the context of a generic SE process.
- Section 3.4, Correlation between the ISSE process and standard examples of SE processes.
- Section 3.5, Relationship of ISSE to DITSCAP.

The generic SE process that forms the basis for describing the ISSE process comprises the following activities:

- Discover Needs.
- Define System Requirements.
- Design System Architecture.
- Develop Detailed Design.
- Implement System.
- Assess Effectiveness

The dependencies (i.e., direction of information flow) between these activities are shown in Figure 3-1. Arrows indicate the flow of information between the activities but not necessarily their sequence or timing. Although not an activity, the Users/Users' Representatives element is a reminder that throughout the process there is continual interaction and feedback between the systems engineer or information systems security engineer and the users.

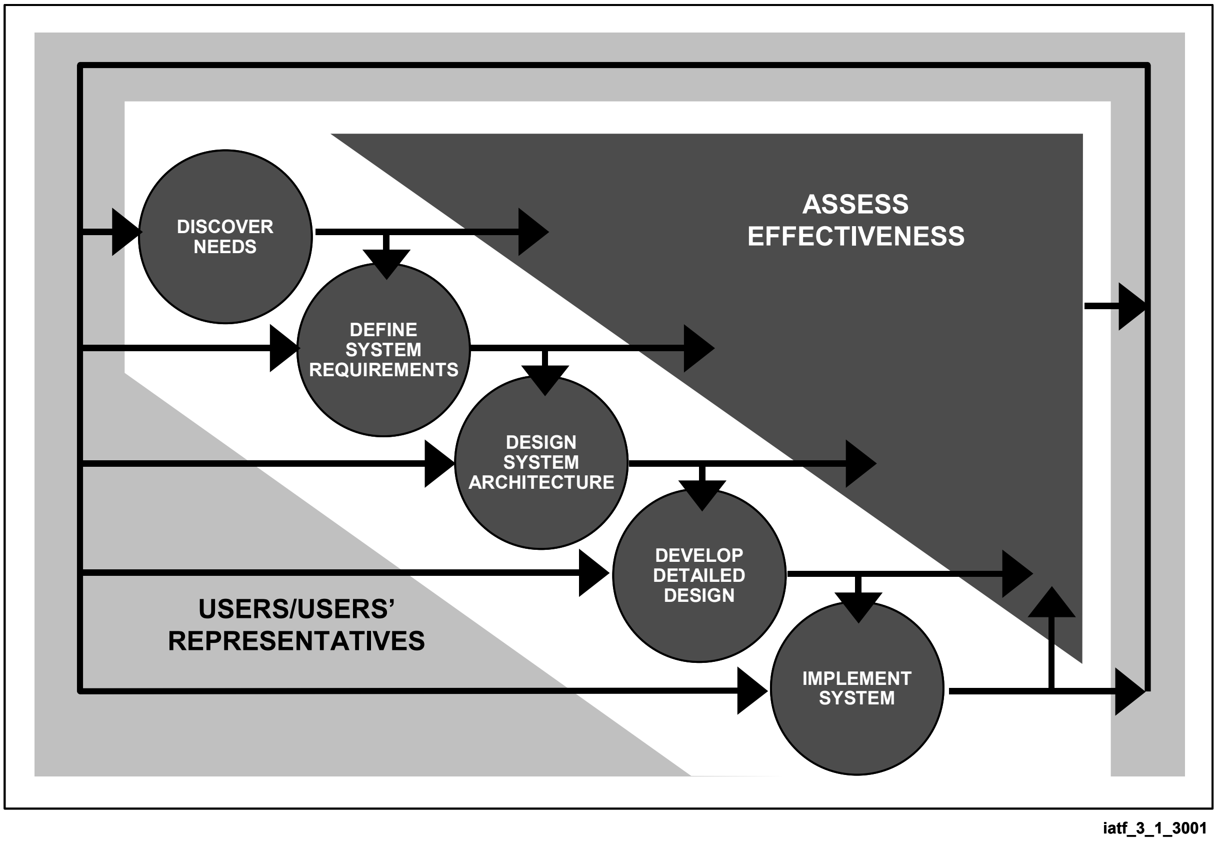


Figure 3-1. Generic Systems Engineering Process

This SE process diagram shown in Figure 3-1 differs from others the reader may have seen in its emphasis on the provision of SE assistance over the entire development life cycle, including needs discovery, system implementation, and assessment of system effectiveness. The Discover Needs activity is often a predecessor to the SE process, rather than a part of that process, because the systems engineer's customer usually performs this activity as part of an acquisition process. However, because information protection needs are seldom identified during the customer's process, Discover Needs and the corresponding ISSE activity, Discover Information Protection Needs, are included here.

Similarly, the Implement System activity is not included in all SE process descriptions because at that stage the focus has changed from engineering to building, integrating, and testing. Nevertheless, configuring the components and the system correctly and training users and administrators are critical to achieving the required information protection; therefore, Implement System and the corresponding ISSE activity, Implement System Security, are included as well.

Most SE processes address system effectiveness issues throughout the development life cycle. In the diagram in Figure 3-1 Assess Effectiveness is explicitly shown to emphasize the interaction with the user organization in establishing mission needs and defining measures-of-effectiveness before designing the system, and in assessing the effectiveness of the system, as designed, developed, and implemented, in satisfying those needs.

All of the ISSE activities that correspond to the SE activities in Figure 3-1 are listed and described in Table 3-1.

Table 3-1. Corresponding SE and ISSE Activities

SE Activities	ISSE Activities
Discover Needs The systems engineer helps the customer understand and document the information management needs that support the business or mission. Statements about information needs may be captured in an information management model (IMM).	**Discover Information Protection Needs** The information systems security engineer helps the customer understand the information protection needs that support the mission or business. Statements about information protection needs may be captured in an Information Protection Policy (IPP).
Define System Requirements The systems engineer allocates identified needs to systems. A system context is developed to identify the system environment and to show the allocation of system functions to that environment. A preliminary system Concept of Operations (CONOPS) is written to describe operational aspects of the candidate system (or systems). Baseline requirements are established.	**Define System Security Requirements** The information systems security engineer allocates information protection needs to systems. A system security context, a preliminary system security CONOPS, and baseline security requirements are developed.
Design System Architecture The systems engineer performs functional analysis and allocation by analyzing candidate architectures, allocating requirements, and selecting mechanisms. The systems engineer identifies components or elements, allocates functions to those elements, and describes the relationships between the elements.	**Design System Security Architecture** The information systems security engineer works with the systems engineer in the areas of functional analysis and allocation by analyzing candidate architectures, allocating security services, and selecting security mechanisms. The information systems security engineer identifies components or elements, allocates security functions to those elements, and describes the relationships between the elements.
Develop Detailed Design The systems engineer analyzes design constraints, analyzes trade-offs, does detailed system design, and considers life-cycle support. The systems engineer traces all of the system requirements to the elements until all are addressed. The final detailed design results in component and interface specifications that provide sufficient information for acquisition when the system is implemented.	**Develop Detailed Security Design** The information systems security engineer analyzes design constraints, analyzes trade-offs, does detailed system and security design, and considers life-cycle support. The information systems security engineer traces all of the system security requirements to the elements until all are addressed. The final detailed security design results in component and interface specifications that provide sufficient information for acquisition when the system is implemented.

SE Activities	ISSE Activities
Implement System The systems engineer moves the system from specifications to the tangible. The main activities are acquisition, integration, configuration, testing, documentation, and training. Components are tested and evaluated to ensure that they meet the specifications. After successful testing, the individual components—hardware, software, and firmware—are integrated, properly configured, and tested as a system.	**Implement System Security** The information systems security engineer participates in a multidisciplinary examination of all system issues and provides inputs to C&A process activities, such as verification that the system as implemented protects against the threats identified in the original threat assessment; tracking of information protection assurance mechanisms related to system implementation and testing practices; and providing inputs to system life-cycle support plans, operational procedures, and maintenance training materials.
Assess Effectiveness The results of each activity are evaluated to ensure that the system will meet the users' needs by performing the required functions to the required quality standard in the intended environment. The systems engineer examines how well the system meets the needs of the mission.	**Assess Information Protection Effectiveness** The information systems security engineer focuses on the effectiveness of the information protection—whether the system can provide the confidentiality, integrity, availability, authentication and nonrepudiation for the information it is processing that is required for mission success.

3.2 Principles

Nothing is more inefficient than solving the wrong problem and building the wrong system. In this section, we discuss three important principles that will help avoid this inefficiency. These principles are—

1. Always keep the problem and solution spaces separate.
2. The problem space is defined by the customer's mission or business needs.
3. The systems engineer and information systems security engineer define the solution space, driven by the problem space.

Principle 1: Always keep the problem and the solution spaces separate.
The problem is *what* we want the system to do. The solution is *how* the system will do what we want it to do. When we focus on the solution, it is easy to lose sight of the problem. This can lead to solving the wrong problem and building the wrong system. As we have noted, *nothing is more inefficient than solving the wrong problem and building the wrong system*.

Principle 2: The problem space is defined by the customer's mission or business needs.
Often customers talk to engineers in terms of technology and their notion of solutions to their problems, rather than in terms of the problem. Systems engineers and information systems security engineers must set these notions aside and discover the customer's underlying problem. If the user requirements are not based on the customer's mission or business needs, the resulting system solution is not likely to respond to those needs. Again, this will lead to building the wrong system, and *nothing is more inefficient than solving the wrong problem and building the wrong system*.

Principle 3: The systems engineer and information systems security engineer define the solution space, driven by the problem space.
The systems engineer, not the customer, is the expert on system solutions. If the customer were the design expert, there would be no need to hire the systems engineer. A customer who insists on intervening in the design process may place constraints on the solution and limit the flexibility of the systems engineer in developing a system that supports the mission or business goals and meets the users' requirements.

In summary, the customer owns the problem. It is the customer's mission or business that the system is intended to support. However, the customer is not always the expert in discovering and documenting the problem. The engineers should help the customer with discovering and documenting the problem. At the same time the systems engineer, not the customer, is the expert in designing solutions. The systems engineers and information systems security engineers should resist the customer's tendency to intervene in design.

3.3 Process

The ISSE process section covers six activities that correspond to a generic SE process:

- Discover Information Protection Needs (Discover Needs).
- Define System Security Requirements (Define System Requirements).
- Design System Security Architecture (Design System Architecture).
- Develop Detailed Security Design (Develop Detailed Design).
- Implement System Security (Implement System).
- Assess Information Protection Effectiveness (Assess Effectiveness).

The ISSE process and its SE context are described in detail below.

3.3.1 Discover Information Protection Needs

Discover Information Protection Needs is the first activity of the ISSE process. The corresponding SE activity is Discover Needs (see Figure 3-1). If the Discover Needs activity is not being performed or is incomplete, the information systems security engineer must complete the following SE tasks:

- Develop an understanding of the customer's mission or business.
- Help the customer determine what information management is needed to support the mission or business.
- Create a model of that information management, with customer concurrence.
- Document the results as the basis for defining information systems that will satisfy the customer's needs.

To understand the customer's mission or business, information systems security engineers must take advantage of all available source material, such as operational doctrine,[1] Web pages, annual reports, and proprietary documentation. The mission or business may be summarized in documents such as a mission needs statement (MNS) or a high-level version of a Concept of Operations (CONOPS), but the most important source of information is direct contact with the customer.

Underlying the customer's mission or business is the information management that supports operations. The first operational elements a customer will think of are the products and services the operation provides, but systems engineers must also seek other important support functions, such as command and control, logistics, human resources, finance, research and development, management, marketing, and manufacturing.

To define information management needs, a model is developed that identifies processes, the information being processed, and the users of the information and the processes. This modeling is in effect a structured analysis that decomposes user roles, processes, and information until ambiguity is reduced to a satisfactory degree. An important step in this modeling is to apply "least privilege" rules, by which users are limited to the processes and information they need to do their jobs. The model should also include the requirements of any information management policies, regulations, and agreements that apply to the information being managed. The main components of the model are information domains, each of which identifies three elements:

- Users or members of the information domain.
- Rules, privileges, roles, and responsibilities that apply to the users in managing all the information.
- Information objects being managed, including processes.

The model, then, is a collection of information domains. The resulting document, the IMM, is usually a very detailed representation of information management needs. The information systems security engineer may support the systems engineer in developing the IMM. This part of the Discover Information Protection Needs activity is presented in detail in the protection needs elicitation (PNE) appendix to this IATF. See Figure 3-2 for an illustration of Discover Information Protection Needs.

Once the IMM is complete, the information systems security engineer can use this knowledge to identify applicable protection policies, security regulations, directives, laws, etc. These documents may identify required levels of security (for example National Security Agency [NSA] approved cryptography for classified information), or C&A procedures that must be followed.

[1] Operational doctrine, as used here, is a set of documents that describe how an organization conducts its mission. It should not be confused with security doctrine, which is an architectural element that describes secure procedures for systems.

A critical part of the Discover Information Protection Needs activity is defining threats to the information. With the customer as the best source of knowledge, and informed by the information systems security engineer's expertise, each information domain is assigned metrics for harm to information (HTI) and potentially harmful events (PHE). HTI considers the value of the information and the degree of harm to the mission if the information were disclosed, modified, destroyed, or unavailable when needed. PHE considers the existence of malicious adversaries, their degree of motivation, and the potential for accidents and natural disasters. Each information domain then has an HTI and a PHE assigned for disclosure, modification, destruction, and unavailability. The HTIs and PHEs are then combined to produce a single information threat metric, such as 3, 2, 1, and 0, with 0 representing no threat. The actual choice of metrics and the method of combining them must be understandable and acceptable to the customer. One recommendation for choosing and combining these metrics is given in the PNE appendix to the IATF.

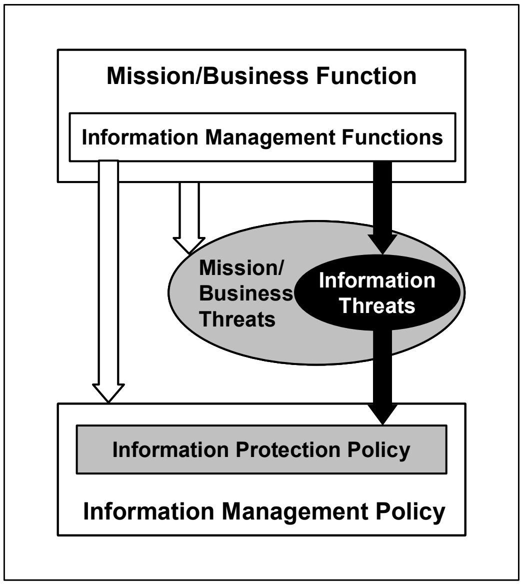

Mission/Business Function
Information Management Functions
Mission/ Business Threats
Information Threats
Information Protection Policy
Information Management Policy
iatf_3_2_0079

Figure 3-2. Discover Needs

The ISSE process defines the security services and the strengths of service using the information threat as a guideline for setting protection priorities. The information systems security engineer and the customer apply confidentiality, integrity, availability, access control, identification and authentication (I&A), nonrepudiation, and security management services, as appropriate to each information threat. The strengths of the services are proportional to the information threat metrics.

Documentation is crucial in all stages of SE and ISSE. In this activity, the information systems security engineer documents information threats; security services, strengths, and priorities; and roles and responsibilities. The information threats and the corresponding security services in the system or systems used to support the customer's mission or business are documented in an IPP. When customer concurrence is obtained, the IPP is assumed to be part of the customer's information management policy. This policy will be the basis for assessing the effectiveness of the information protection throughout the remainder of the process activities. Figure 3-2 illustrates the flow from mission or business to the IPP.

Early in the engineering process, the information systems security engineer also should begin documenting design constraints. These may be found in the legal and regulatory requirements identified earlier or they may be inherited from legacy systems that must interface with the target system. In either case, they must be documented and tracked throughout the SE/ISSE process.

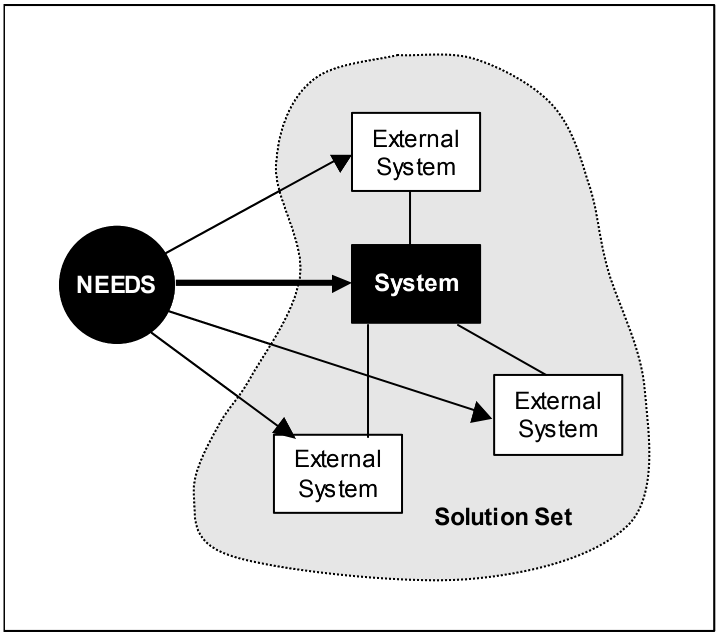
The information systems security engineer is responsible for presenting the process, summarizing the information model, identifying the threats and security services, and determining the threats' and services' relative strengths and priorities to the customer. Since this documents the customer's information management and protection needs, on which all further development efforts will be based, customer agreement on the conclusions reached in this activity is essential and is the measure of the effectiveness of the information systems security engineer's efforts. In each activity of the ISSE process, the information systems security engineer will perform activities to support the C&A of the system. In the Discover Information Protection Needs activity, the focus is on identifying the key roles (i.e., Designated Approving Authority [DAA]/Accreditor and Certification Authority/Certifier) and the process to be used for C&A and acquisition of the system, and on obtaining concurrence in the documented results of this activity, as required.

3.3.2 Define System Security Requirements

In this activity, which is part of the Define System Requirements activity of SE, the information systems security engineer considers one or more solution sets that can meet the information protection needs expressed by the customer and documented in the IPP. The mapping of needs to a solution set is illustrated in Figure 3-3. Each solution set includes a system concept for the target system, which defines the following:

- System context.
- Preliminary CONOPS.
- System requirements (what the system is to accomplish).

With customer involvement, one solution set is chosen and its system context, CONOPS, and requirements are documented. This activity can result in the need to modify existing systems or to develop more than one target system. Figure 3-3 also illustrates the allocation of needs to systems other than the target system. Examples of external systems include a system that provides a Public Key Infrastructure (PKI) and a system for security clearances of users.



iatf_3_3_0080

Figure 3-3. Allocation of Needs into a Solution Set

Developing the system security context involves defining system boundaries and interfaces with SE, allocating security functions to target or external systems, and identifying data flows between the target and external systems and protection needs associated with those flows. Information management needs (per the IMM) and information protection needs (per the IPP) are allocated to the target system and to external systems; allocations to external systems are assumptions that must be accepted by these systems' owners. The system security context documents those allocations and specifies data flows between the system and external systems and how they are controlled.

A preliminary security CONOPS describes, from a user perspective, what information management and information protection functions the system will perform in support of the mission, but falls short of defining step-by-step procedures. The CONOPS will define the reliance of mission or business needs on other systems and the products and services they deliver. The system security context and CONOPS are coordinated with the systems engineer, the customer, and owners of external systems.

The information systems security engineer works with the systems engineers to define system security requirements, system security modes of operation, and system security performance measures. Good system requirements specify what a system must do, without specifying its design or implementation. The systems engineer and the information systems security engineer must ensure that the requirements are understandable, unambiguous, comprehensive, complete, and concise. Requirements analysis must clarify and define functional requirements and design constraints. Functional requirements define quantity (how many), quality (how good), coverage (how far), timelines (when and how long), and availability (how often). Any performance requirements and residual design constraints are carried forward as part of the system requirements document. Design constraints are not independent of implementation but represent design decisions or partial system design. In system requirements documents, design constraints should be identified separately from system interface requirements, which must be documented, including any that are imposed by external systems. Design constraints define factors that limit design flexibility, such as environmental conditions or limits; defense against internal or external threats; and contract, customer, or regulatory standards. When the system requirements are approved, they are documented to give designers a baseline for system development.

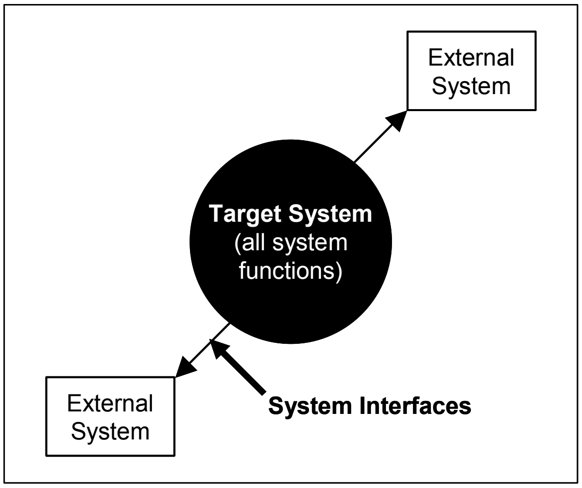
In analyzing requirements, the systems engineer reviews the traceability documentation to ensure that all of the needs discovered have been allocated either to the target system or to external systems and that the context for the target system describes all external interfaces and flows. The systems engineer also ensures that the preliminary system CONOPS covers all of the functionality, missions, or business needs and addresses the inherent risk in operating the system.

The information systems security engineer ensures that the selected solution set meets the mission or business security needs, coordinates the system boundaries, and ensures that the security risks are acceptable. The information systems security engineer will present security context, security CONOPS, and system security requirements to the customer and gain concurrence.

All documentation of the system concept and any rationale for choosing that concept are delivered in compliance with the C&A process. The information systems security engineer is responsible for ensuring that Accreditor and Certifier concurrence is obtained as necessary.

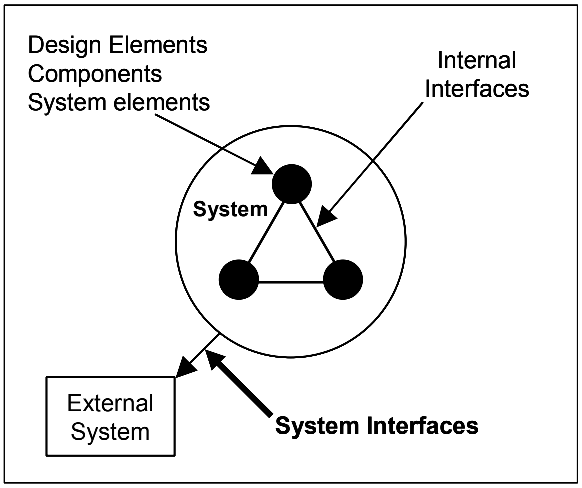
3.3.3 Design System Security Architecture

In the Define System Requirements SE activity, requirements were allocated to an entire information system, indicating the functions to be performed without any definition of system components. In Design System Architecture, the SE team now does functional decomposition, choosing the types of components that will perform specific functions. This process is the core of designing an architecture. Figures 3-4a and 3-4b illustrate the contrast between these two SE activities where Define System Requirements treats the target system as a "black box" and Design System Architecture creates the structure within the system. The same contrast occurs in the corresponding ISSE activities—Define System Security Requirements and Design System Security Architecture.



iatf_3_4a_3004a

Figure 3-4a. Define System Requirements



iatf_3_4b_3004b

Figure 3-4b. Design System Architecture

Functions are analyzed by decomposing higher-level functions identified through requirements analysis into lower level functions. The performance requirements associated with the higher level are allocated to lower level functions. The result is a description of the product or item in terms of what it does logically and in terms of the performance required. This analysis includes candidate system architectures, function and process, interfaces (internal and external), elements (components), information transfers, environments, and users/accesses.

This description is often called the functional architecture of the product or item. Functional analysis and allocation allow a better understanding of what the system has to do; the ways in which it can do it; and to some extent, the priorities and conflicts associated with lower level functions. It provides information essential to optimizing physical solutions. Key tools in functional analysis and allocation are Functional Flow Block Diagrams, Timeline Analysis, and the Requirements Allocation Sheet.

During this task, the information systems security engineer works with the systems engineers to ensure that security requirements flow properly to the architecture and that architecture decisions do not impede security.

The information systems security engineer works to allocate security requirements to the target and external systems and to ensure that external systems identified can support what is allocated to them. This is particularly important for security, since services such as key management are often allocated to external systems.

The information systems security engineer will identify high-level security mechanisms during this task (e.g., encryption, digital signature). This is necessary so that dependencies, such as key management for encryption, can be addressed and allocated. The information systems security engineer should match mechanisms to security service strength, apply design constraints, analyze and document shortfalls, perform interdependency analysis, ascertain the feasibility of mechanisms, and assess any residual risk associated with the mechanisms. Specific implementations of the security mechanisms are not identified in the architecture, so detailed vulnerability and attack information is not available to support the formal risk analysis process. However, an experienced information systems security engineer can describe the expected vulnerabilities in potential components and can develop attack scenarios to use in the risk analysis process.

The risk analysis process ensures that the selected security mechanisms provide the required security services and helps explain to the customer how the security architecture meets the security requirements. The effectiveness of the architecture in meeting these requirements is based on the results of the risk analysis and whether the customer concurs with the recommended course of action at this stage of development.

The information systems security engineer supports C&A by coordinating the security architecture and the results of the risk analysis with the Accreditor and the Certifier.

3.3.4 Develop Detailed Security Design

The development of the information protection design is iterative, involving interactions between the SE and ISSE teams and between systems and component engineers within the teams. Decisions leading to the recommended design involve continuous assessments by the ISSE team to compare the expected risk with the system security requirements. The system security requirements set priorities for protection that the ISSE team applies accordingly. The ISSE team produces the design documentation required by the C&A process. That documentation enables independent evaluation of the design by risk analysts who then provide feedback on vulnerabilities.

In Develop Detailed Security Design, the information systems security engineer will ensure compliance with the security architecture, perform trade-off studies, and define system security design elements, including—

- Allocating security mechanisms to system security design elements.
- Identifying candidate commercial off-the-shelf (COTS)/government off-the-shelf (GOTS) security products.
- Identifying custom security products.

- Qualifying element and system interfaces (internal and external).
- Developing specifications (e.g., Common Criteria protection profiles).

The information protection design specifies the system and its components, but does not decide on specific components or vendors. The selection of specific components is part of the Implement System activity.

Some important aspects of the ISSE effort are as follows:

- Components include both technical and nontechnical mechanisms (e.g., doctrine).
- Design must satisfy customer-specified design constraints.
- Trade-offs must consider priorities, cost, schedule, performance, and residual security risks.
- Risk analysis must consider the interdependency of security mechanisms.
- Design documents should be under strong configuration control.
- Failures to satisfy security requirements must be reported to C&A authorities.
- Design should be traceable to the security requirements.
- Design should project the schedule and cost of long-lead items and life-cycle support.
- Design should include a revised security CONOPS.

In Develop Detailed Security Design, the information systems security engineer also reviews how well the selected security services and mechanisms counter the threats identified in the IPP by performing an interdependency analysis to compare desired to effective security service strengths. Once completed, the risk assessment results, particularly any identified mitigation needs and residual risk, are documented and shared with the customer to obtain concurrence.

3.3.5 Implement System Security

The objective of the Implement System SE activity is to acquire, integrate, configure, test, document, and train. Implement System moves the system from design to operations. This activity concludes with a final system effectiveness assessment in which evidence is presented that the system complies with the requirements and satisfies the mission needs. Issues across all SE primary functions must be considered and any interdependency or trade-off issues resolved.

During Implement Systems Security, the information systems security engineer provides—

- Inputs to C&A process activities.
- Verification that the system as implemented does protect against the threats identified in the original threat assessment.

- Tracking of, or participation in, application of information protection assurance mechanisms related to system implementation and testing practices.
- Inputs to and review of evolving system life cycle support plans, operational procedures, and maintenance training materials.
- A formal information protection assessment in preparation for the final system effectiveness assessment.
- Participation in the multidisciplinary examination of all system issues.

These efforts and the information each produces support the final system effectiveness assessment. Security accreditation approval typically occurs shortly after the conclusion of the final system effectiveness assessment.

Selecting specific products for integration into the security solution is part of the Implement System Security activity. These products can be acquired by purchase, lease, or borrowing. Selection will be based on factors such as cost of the component, availability, form, and fit. Other factors may include components affect on reliability of the particular system, risk to system performance if component performance is marginal, and future availability of the component or substitutes. Components that cannot be procured must be built. Whether software, hardware, or firmware, components should be verified as corresponding to the design specifications, and the verification must be formally documented. Any deviation must be evaluated for impact on the achievement of design and mission or business objectives, including security.

Components, whether procured or built, must be integrated into the system as designed, and any incompatibility with existing components resolved. Systems are often a hybrid of procured and built components that may need "glue," such as software or interface cabling. During installation and configuration, functions that are needed should be implemented and functions that are not needed for the mission should be restricted.

The information systems security engineer must verify that the evaluation criteria for the security components measure the desired level of security and that the security components meet those criteria. Products may have been evaluated against Commercial COMSEC Evaluation Program (CCEP), National Information Assurance Partnership (NIAP), Federal Information Processing Standards (FIPS), or other NSA and National Institute of Standards and Technology (NIST) criteria.

The ISSE team helps configure the components to ensure that the security features are enabled and the security parameters are set to provide the required security services. Once the system is ready to be configured, any differences in settings that are necessary must be recorded and approved following configuration management procedures.

The systems and design engineers will write test procedures reflecting the results expected as the design solution becomes defined. As components are acquired, they should be unit tested. Verification of the design and interfaces ensures that the produced component operates correctly.

Procedures must test all of the interfaces. If the system is unique or is to be operated in an environment that is difficult to model, however, it may not be possible to fully test all interfaces until the system is installed.

Integration testing verifies subsystem and system performance. Planning for testing should consider the people, tools, facilities, schedule, and capital resources required to test both individual components and the entire system. As components are integrated into the system and tested to ensure that the subsystems and the system are functional, some components may have to be changed. Test reports should document both positive and negative results of the testing.

Design documentation and experience in implementing a system are sources of material for training users and administrators. All documentation should be under strict version control. Training materials and instruction should address operational policy as it pertains to the system and should deal with system limitations as well as functions.

As the system is integrated and tested, it is important to document installation, operation, maintenance, and support procedures. These procedures will be based on the requirements, architecture, design, and test results of the system "as-built" configuration. As installation proceeds, it is important to document defects in the procedures and to note how changes may affect function and mission objectives. The impact of installation changes on the residual risk associated with operating, supporting, and maintaining the system should also be assessed.

The information systems security engineer will develop the information protection-related test plans and procedures and may have to develop test cases, tools, hardware, and software to exercise the system adequately. ISSE activities to this end include—

- Participation in the testing of protection mechanisms and functions.
- Tracking and applying information protection assurance mechanisms related to system implementation and testing practices.
- Providing inputs to and review of evolving life-cycle security support plans, including logistics, maintenance, and training.
- Continuing risk management.
- Supporting the C&A processes.

The information systems security engineer monitors the system security aspects of interfaces, integration, configuration, and documentation. System test and evaluation may reveal unexpected vulnerabilities; the risks and possible mission impacts associated with these vulnerabilities must be evaluated. The results are fed back to the design engineers in an iterative process. The information systems security engineer coordinates with the Certifiers and Accreditors to ensure the completeness of the required documentation. The information systems security engineer also monitors tasks to ensure that the security design is implemented correctly. To accomplish this, he or she will observe and participate in testing and analyze test and evaluation results.

During this task, the risk analysis will be initially conducted or updated. Strategies will be developed to mitigate identified risks and the information systems security engineer will identify possible mission impacts and advise the customer and the customer's Certifiers and Accreditors.

The information systems security engineer ensures that the documentation necessary for C&A is completed and delivered. This documentation will include integration and test reports showing any variations to specifications. The information systems security engineer may contribute to and review these documents.

The ISSE team helps ensure that adequate training material is available for security training. Users must be advised of threats to the operation. Threat information and security responsibilities should be part of the system doctrine and any operational security policy.

3.3.6 Assess Information Protection Effectiveness

The Assess Information Protection Effectiveness activity spans the entire SE/ISSE process. Therefore, it is discussed in each of the preceding activity sections, as appropriate. A summary of the effectiveness assessment tasks related to the various other ISSE activities is provided in Table 3-2.

Table 3-2. Assess Information Protection Effectiveness Tasks by ISSE Activity.

ISSE Activity	Assess Information Protection EffectivenessTask
Discover Information Protection Needs	• Present an overview of the process. • Summarize the information model • Describe threats to the mission or business through information attacks • Establish security services to counter those threats and identify their relative importance to the customer. • Obtain customer agreement on the conclusions of this activity as a basis for determining system security effectiveness.
Define System Security Requirements	• Ensure that the selected solution set meets the mission or business security needs. • Coordinate the system boundaries. • Present security context, security CONOPS, and system security requirements to the customer and gain their concurrence. • Ensure that the projected security risks are acceptable to the customer.
Design System Security Architecture	• Begin the formal risk analysis process to ensure that the selected security mechanisms provide the required security services and to explain to the customer how the security architecture meets the security requirements.
Develop Detailed Security Design	• Review how well the selected security services and mechanisms counter the threats by performing an interdependency analysis to compare desired to effective security service strengths. • Once completed, the risk assessment results, particularly any mitigation needs and residual risk, will be documented and shared with the customer to obtain their concurrence.

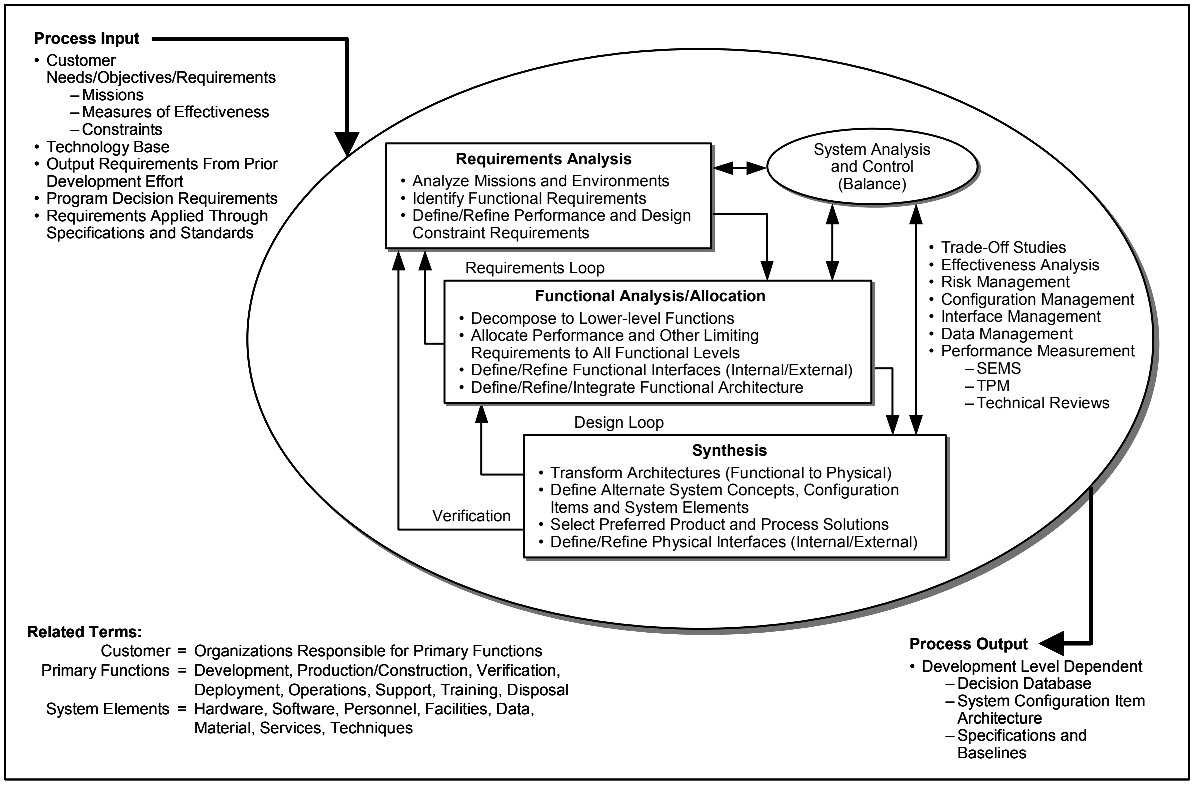
ISSE Activity	Assess Information Protection EffectivenessTask
Implement System Security	• The risk analysis will be conducted/updated. • Strategies will be developed for the mitigation of identified risks • Identify possible mission impacts and advise the customer and the customer's Certifiers and Accreditors.

3.4 ISSE Relationship to Sample SE Processes

The ISSE process description in Section 3.3 used a generic SE process to provide context. This section relates the ISSE activities to two specific systems engineering and acquisition processes, DoD 5000.2-R; Mandatory Procedures for Major Defense Acquisition Programs (MDAP) and Major Automated Information System (MAIS) Acquisition Programs, and the IEEE Standard for Application and Management of the Systems Engineering Process (IEEE Std. 1220-1998). The purpose of this mapping, summarized here and presented in detail in Appendix J, ISSE Relationship to Sample SE Processes, is to help the reader who is familiar with these or similar processes to have a better understanding of the nature of the ISSE activities and of the SE skills involved. Appendix J also includes the ISSE Master Activity and Task List, which is a decomposition of the ISSE process activities into tasks and subtasks. Besides the six technical process activities, two program management activities are included: Plan Technical Effort and Manage Technical Effort. This list is used to map ISSE activities to SE processes.

However, information systems security engineers are cautioned to avoid using this mapping as the sole guide for aligning ISSE activities with a customer's SE activities. When tailoring ISSE activities to specific project timelines, it is important to consider the technical and funding milestones where the future direction of the project will be decided and to ensure that the decision-makers have the security-relevant information to make those decisions. The information systems security engineer must also consider that important activities and milestones may have occurred before the ISSE process was applied, but because of the dependency between activities, all the ISSE activities must be performed to the extent required to support subsequent decisions. For example, the specification and assessment of security components are dependent on system security architecture and detailed system design and the final assessment of information protection effectiveness must be based on an understanding of the information protection needs.

DoD 5000.2-R, MDAPs and MAIS Acquisition Programs, describe the Systems Engineering Process (SEP) as a comprehensive, iterative, and recursive problem-solving process, applied sequentially, top down. Figure 3-5 presents a diagram of this process:


Process Input
• Customer Needs/Objectives/Requirements
– Missions
– Measures of Effectiveness
– Constraints
• Technology Base
• Output Requirements From Prior Development Effort
• Program Decision Requirements
• Requirements Applied Through Specifications and Standards
Requirements Analysis
• Analyze Missions and Environments
• Identify Functional Requirements
• Define/Refine Performance and Design Constraint Requirements
System Analysis and Control (Balance)
Requirements Loop
Functional Analysis/Allocation
• Decompose to Lower-level Functions
• Allocate Performance and Other Limiting Requirements to All Functional Levels
• Define/Refine Functional Interfaces (Internal/External)
• Define/Refine/Integrate Functional Architecture
• Trade-Off Studies
• Effectiveness Analysis
• Risk Management
• Configuration Management
• Interface Management
• Data Management
• Performance Measurement
– SEMS
– TPM
– Technical Reviews
Design Loop
Synthesis
• Transform Architectures (Functional to Physical)
• Define Alternate System Concepts, Configuration Items and System Elements
• Select Preferred Product and Process Solutions
• Define/Refine Physical Interfaces (Internal/External)
Verification
Related Terms:
Customer = Organizations Responsible for Primary Functions
Primary Functions = Development, Production/Construction, Verification, Deployment, Operations, Support, Training, Disposal
System Elements = Hardware, Software, Personnel, Facilities, Data, Material, Services, Techniques
Process Output
• Development Level Dependent
– Decision Database
– System Configuration Item Architecture
– Specifications and Baselines

iatf_3_5_3003

Figure 3-5. DoD 5000.2-R Systems Engineering Process

Figure 3-6 shows a diagram of IEEE Std 1220-1998.

3.5 Relationship of ISSE to DITSCAP

This section discusses the relationship of ISSE to DITSCAP. In general, the discussion also applies to ISSE's relationship to other C&A processes.

The ISSE process helps the customer discover information protection needs to support the customer's mission or business and helps build a system to meet those needs. Much of the information and analysis required by C&A processes can be gathered from the results of the ISSE process. Throughout these activities, the information systems security engineer works in support of the systems engineer, but must also satisfy the DAA.

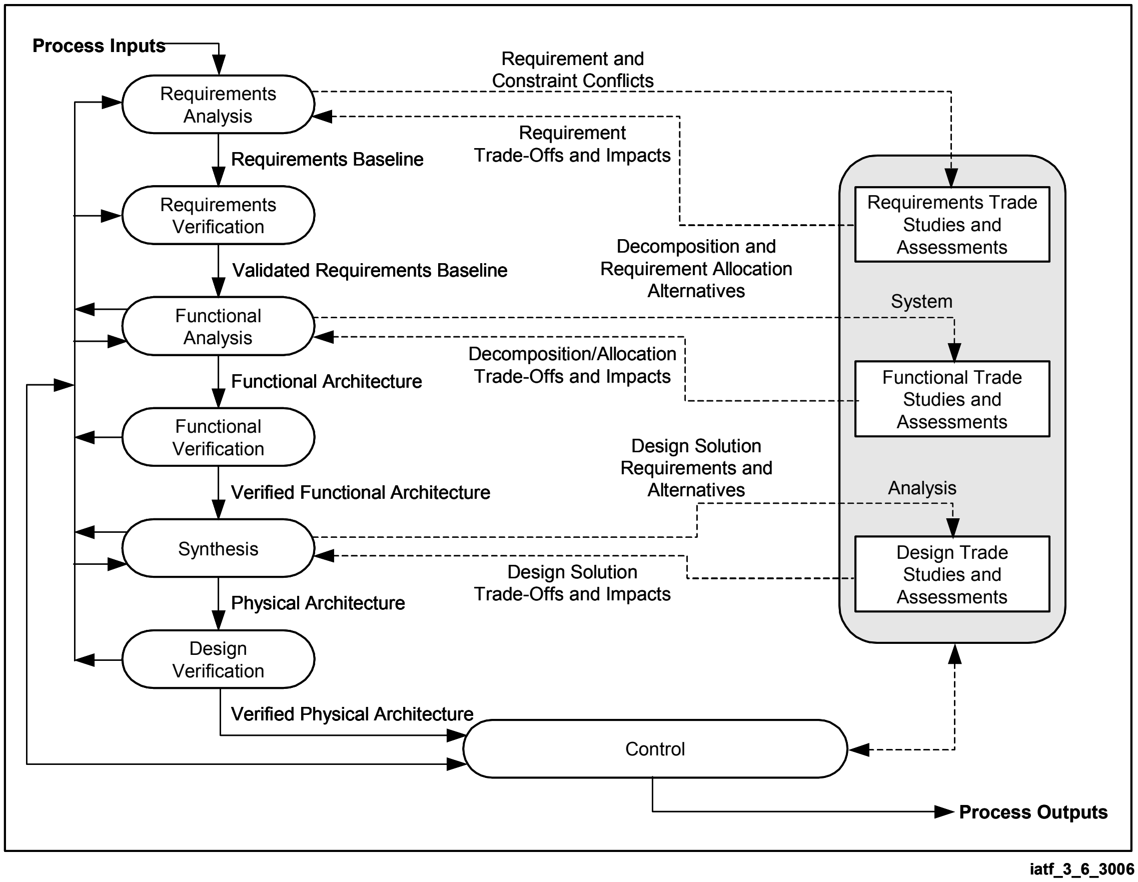

Process Inputs
Requirements Analysis
Requirement and Constraint Conflicts
Requirement Trade-Offs and Impacts
Requirements Baseline
Requirements Verification
Requirements Trade Studies and Assessments
Validated Requirements Baseline
Decomposition and Requirement Allocation Alternatives
System
Functional Analysis
Decomposition/Allocation Trade-Offs and Impacts
Functional Architecture
Functional Trade Studies and Assessments
Functional Verification
Design Solution Requirements and Alternatives
Verified Functional Architecture
Analysis
Synthesis
Design Solution Trade-Offs and Impacts
Design Trade Studies and Assessments
Physical Architecture
Design Verification
Verified Physical Architecture
Control
Process Outputs
iatf_3_6_3006

Figure 3-6. IEEE Std 1220-1998 Systems Engineering Process

DITSCAP establishes a C&A process and sets out activities for collecting and evaluating evidence that will lead to the accreditation of an information system that meets the security requirements needed to support the customer's mission or business. DITSCAP is a process for certifying that the information system not only meets documented security requirements but also will continue to do so. The key to the DITSCAP is the agreement between the information system's program manager, the DAA, the Certifier, and the user's representative. This agreement is documented in the System Security Authorization Agreement (SSAA).

Figure 3-7 shows that the development (SE/ISSE) process and the C&A process are separate, but related processes with distinct roles and outcomes. The SE/ISSE process results in system implementation and documentation; the C&A process results in certification documentation, a certification recommendation, and an accreditation decision. The SE/ISSE process produces evidence and documentation used by the C&A process. The C&A process provides feedback used by the SE/ISSE process. Both processes have one thing in common—the ultimate goal of an operational system that supports the user organization's mission or business.

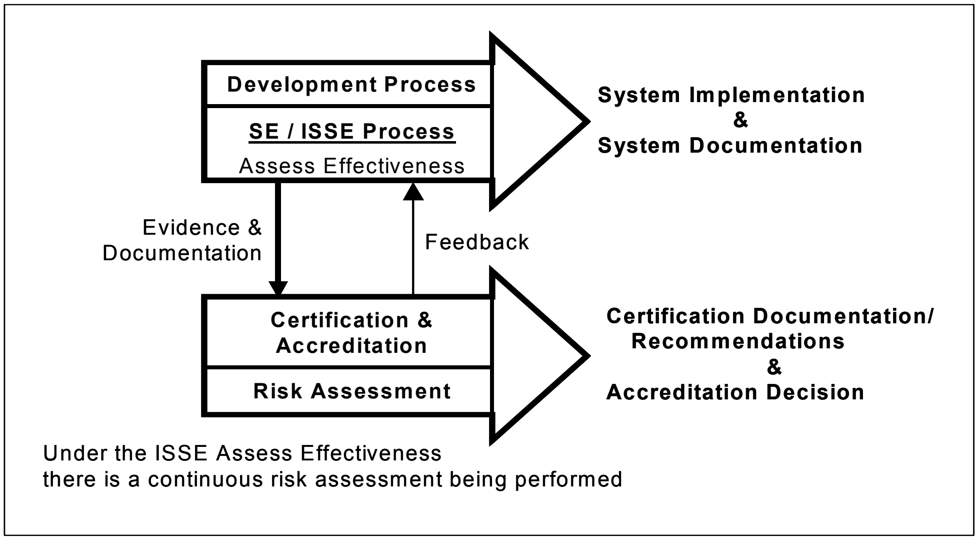


Figure 3-7. Relationship of SE/ISSE and C&A

DITSCAP is not a design process. It does not provide information on how to discover requirements or how to design, implement, or evaluate a system. It establishes only what evidence must be collected for an evaluation and that an evaluation must be performed.

In a system development effort in which SE/ISSE was not applied, the evidence and documentation required for C&A may not be available. The certification team may have to retroactively generate this information when they initiate certification efforts after some or all of the development effort is complete. There are four phases in the DITSCAP: Definition, Verification, Validation, and Post-Accreditation.

Phase 1, Definition, documents the information protection requirements, the system's context, and the system architecture. The resulting documents are collected and evaluated for completeness. This phase also identifies the level of effort required to achieve accreditation, the Certification Authority (Certifier), and the DAA. The three activities in the Definition phase are preparation, registration, and negotiation. In the preparation activity, information and documentation about the system are collected and reviewed. The types of information collected may include the following:

- Business case.
- MNS.
- System specifications.
- Architecture and design documents.
- User manuals.
- Operating procedures.
- Network diagrams.
- Configuration management documents.
- Threat analysis.

Typically, this information can be found in system specifications, and the architecture and design documentation generated by the SE/ISSE process in system development.

In the registration activity, the information collected during preparation is evaluated and documented in the SSAA. The tasks that must be performed [2] during registration are as follows:

- Prepare business or operational functional description and system identification.
- Inform the DAA, the Certifier, and the user's representative that the system will require C&A support (register the system).
- Prepare the environment and threat description.
- Prepare system architecture description and describe the C&A boundary.
- Determine system security requirements.
- Tailor the DITSCAP tasks, determine the C&A level of effort, and prepare a DITSCAP plan.
- Identify organizations that will be involved in the C&A and identify the resources required.
- Develop the draft SSAA.

In the negotiation activity, agreement is reached between the program manager, the DAA, the Certifier, and the user's representative on the approach, security requirements, level of effort required for the C&A activities, and schedule. The tasks that must be performed during negotiation are—

- Conduct the certification requirements review.
- Agree on the security requirements, level of effort, and schedule.
- Approve final Phase 1 SSAA.

The ISSE process is the source of many of the documents required in Phase 1, Definition, among them—

- The IPP, written during Discover Information Protection Needs, provides the mission information threat analysis, the information protection requirements needed to counter the identified threats, and the customer's prioritization of the requirements. In addition, the IPP documents who the Certifier and the DAA for the system are.
- The security context, generated during Define System Security Requirements, sets the system boundary and identifies external interfaces to the system.
- The security architecture, developed during Design System Security Architecture.

[2] The system engineer, information systems security engineer, or developer, under the direction of the program manager, most often performs these tasks. The certifier is responsible for the content of the SSAA. The DAA approves the SSAA.

In Phase 2, Verification, documents are collected on the system as designed and implemented. These documents are used to evaluate system compliance with the security requirements and constraints identified in the SSAA. The following tasks must be performed[3] during Verification:

- System architecture analysis.
- Software design analysis.
- Network connection rule compliance analysis.
- Integrity analysis of integrated products.
- Life-cycle management analysis.
- Preparation of security requirements validation procedures.
- Vulnerability assessment.

The output of the ISSE Design System Security Architecture, Develop Detailed Security Design, Implement System Security, and Assess Information Protection Effectiveness activities are the source of many of the documents and much of the analysis required in Phase 2. For example—

- Doctrine from the security architecture in Design System Security Architecture.
- The security design developed in Develop Detailed Security Design.
- The security design analysis from Develop Detailed Security Design
  - Hardware
  - Software
  - Firmware.
- The security configuration from Develop Detailed Security Design.
- Implementation documentation from Implement System Security (e.g., security integration test plans).

Phase 3, Validation, ensures that the implemented design operates in a specific operating environment with an acceptable level of risk. The activities in this phase begin with system integration and end with accreditation of the system. The following are the tasks that, if required,[4] are performed[5] during Validation:

- Security Test and Evaluation (ST&E).
- Penetration testing.
- TEMPEST and Red-Black evaluation.
- COMSEC compliance evaluation.
- System management analysis.
- Site accreditation survey.
- Contingency plan evaluation.
- Risk management review.

[3] Certifiers and evaluators most often perform these tasks. SE and ISSE support these tasks.

[4] As an example, TEMPEST may not be a requirement if the system is within the continental United States.

[5] Certifiers and evaluators most often perform these tasks with SE and ISSE support.

The output of the ISSE activities Develop Detailed Security Design, Implement System Security and Assess Information Protection Effectiveness are the source of much of the input that is required in Phase 3. For example—

- During the Develop Detailed Security Design activity, the information systems security engineer either writes or provides input to detailed security test plans, such as an ST&E. During Implement System Security, the information systems security engineer supports and analyzes the results of those tests.
- During Implement System Security and Assess Information Protection Effectiveness, the information systems security engineer provides support to any ongoing risk management activities.

Phase 4, Post-Accreditation, contains the activities required to continue to operate and manage the system so that it will maintain an acceptable level of risk. Phase 4 begins once the system has been accredited. With any major changes to the system, DITSCAP reverts to Phase 1. The tasks performed under Phase 4 are as follows:

- SSAA maintenance.
- Physical, personnel, and management control review.
- TEMPEST evaluation.
- COMSEC compliance evaluation.
- Contingency plan maintenance.
- Configuration management.
- System security management.
- Risk management review.

If DITSCAP reverts to Phase 1, the support from ISSE is provided as described in the previous paragraphs.

3.6 Summary

This chapter provides an overview of the ISSE process followed by discussion of four main topics: SE and ISSE principles, the ISSE process, a correlation between sample SE processes and the ISSE process, and the relationship of the ISSE process to DITSCAP.

The three SE and ISSE principles are—

1. Always keep the problem and the solution spaces separate.
2. The problem space is defined by the customer's mission or business needs.
3. The systems engineer and information systems security engineer define the solution space, driven by the problem space.

The summary of these principles emphasizes that the customer owns the problem—it is the customer's mission or business that the system is intended to support. Though the customer owns the problem, the customer is not always the expert in discovering and documenting it, and here the systems engineer or information systems security engineer should help. The systems engineer and the information systems security engineer and not the customer are the experts in developing solutions. The systems engineer and the information systems security engineer should resist the customer's tendency to intervene in the design of the system. Customer design inputs could become constraints on the final design and limit the SE design flexibility.

The ISSE process section covers six activities that correspond to a generic SE process:

- Discover Information Protection Needs (Discover Needs).
- Define System Security Requirements (Define System Requirements).
- Design System Security Architecture (Design System Architecture).
- Develop Detailed Security Design (Develop Detailed Design).
- Implement System Security (Implement System).
- Assess Information Protection Effectiveness (Assess Effectiveness).

Each activity stresses the importance of interaction with the customer. The National Cryptologic School (NCS) offers courses on the SE/ISSE process:

- IAEC3186 *Introduction to ISSE.*
- IAEC3341 *Protection Needs Elicitation.*

The third topic in this chapter shows the similarities between the ISSE process and two standard SE processes, DoD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAP) and Major Automated Information System (MAIS) Acquisition Programs, and the IEEE Standard for Application and Management of the Systems Engineering Process.

The relationship between the ISSE process and DITSCAP is best summarized in Figure 3-7. The figure shows that the development (SE/ISSE) process and the C&A process are separate. The SE/ISSE process results in system implementation and system documentation. The C&A process results in certification documentation, a certification recommendation, and an accreditation decision. The SE/ISSE process produces evidence and documentation used by the C&A process. The C&A process provides feedback used by the SE/ISSE process. This section also points out that DITSCAP is a C&A process and not a design process.

References

1. IAEC3341. Protection Needs Elicitation (PNE), Session 01-02, October 2001.
2. DoD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs), and Major Automated Information System Acquisition Programs (MAIS).
3. DoD Directive 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 November 1997.
4. IAEC3186. Introduction to Information Systems Security Engineering (ISSE), Session 02-01, September 2001.
5. IEEE Standard for Application and Management of the Systems Engineering Process (IEEE Std 1220-1998).